REMARKS

Claims 13-15 and 17-25 are currently pending. By this amendment, claims 13, 19, and 21 have been amended, claim 16 has been canceled, and new claim 25 has been added.

Telephonic Interview

Applicants wish to thank the Examiner and his supervisor for an Examiner's Interview conducted on 02 September 2010. While no agreement was reached, the Examiner suggested filing a Response including the additional arguments and agreed to reconsider the rejection of claims 13-24 under 35 U.S.C. § 103(a), as allegedly being obvious over U.S. Patent No. 6,282,522 issued to Davis et al. (hereinafter "Davis") in view of U.S. Patent No. 6,847,953 issued to Kuo (hereinafter "Kuo") and further in view of Published U.S. Patent Application No. 2002/0133468 filed by Mertens (hereinafter "Mertens").

As discussed during the interview, the methods disclosed in Davis, Kuo, and Mertens differ significantly from one another and combining them as suggested by the Office Action requires the application of impermissible hindsight. In the interest of advancing prosecution, however, independent claim 13 has been amended to clarify differences between the claimed invention and these references.

Davis

Turning now to the cited references, referring to Figure 4 (reproduced below), Davis discloses an architecture 200 for an internet payment system involving a smart card (column 10, lines 32-34). A client terminal 204 controls the interaction with a user and interfaces with a card reader 210 that accepts a smart card 5 having a stored-value application (column 10, lines 50-52). A payment server 206 communicates directly with a terminal or through a concentrator 212 that handles any number of terminals 214-216 each having a security card 218 and 220, respectively (column 10, lines 54-58). The security cards 218 and 220 each authenticate and validate stored-value cards (column 11, lines 48-52). The payment server 206 also communicates with concentration point 68 for transmission of transaction data to a clearing and administration system (column 10, lines 58-60). A merchant server 208 is a site that has contracted with an acquirer to

accept stored-value card transactions as payments for goods and/or services purchased over the Internet (column 10, lines 63-65).

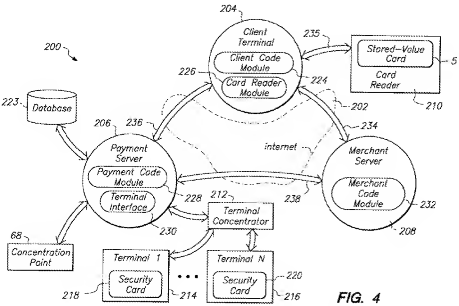


FIG. 4

During a financial transaction, the client terminal 204 and merchant server 208 exchange information 234 via internet 202 (column 13, lines 56-58). The merchant server 208 generates a unique identification of the transaction, and builds an HTML page and sends it to the client terminal 204 (column 13, lines 63-67). The client terminal 204 interacts with the stored-value card 5 and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server (column 13, line 67, to column 14, line 3). The client terminal 204 forwards the draw request to the payment server 206 (column 14, lines 4-6).

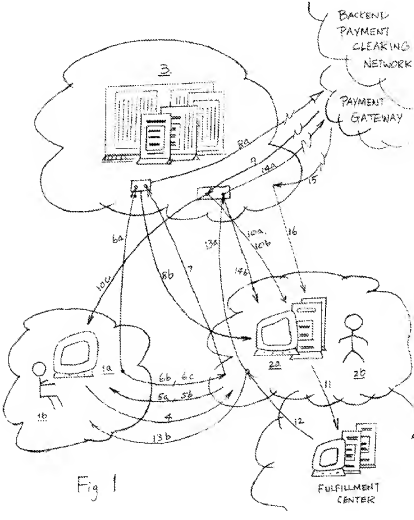
After determining the transaction is a valid transaction from a known merchant, the payment server 206 builds a message (with a debit command) containing the identification of the transaction and signs it with a security card signature 314 from the security card 220 in the terminal 216 (column 14, lines 6-11, and column 16, lines 64-67). The message is routed to the client terminal 204, which passes the debit command and security card signature 314 to stored-value card 5 which verifies the signature, and debits itself by the purchase amount (column 17,

lines 12-14). The stored-value card 5 sends a success message 320 (see Figure 5) along with the card signature back to the client terminal 204, which packages the success message along with the card signature and sends them back to payment server 206 (column 17, lines 34-42). The client terminal 204 passes a confirmation message 330 (see Figure 5) to the merchant server 208 (column 18, lines 40-43). The merchant server 208 validates the confirmation message 330 (column 18, lines 47-55). If the validation is successful, the merchant server determines a successful transaction has occurred. *Id.*

Amended independent claim 13 recites a method of making a financial transaction over the internet. The method includes receiving at a virtual credit card terminal (VCT) gateway a request for a transaction number from a merchant after the merchant has received an indication from a purchaser that the purchaser has elected to pay for selected items from the merchant by credit card means. Further, the method includes receiving a VCT transaction request at the VCT gateway from the purchaser, the VCT transaction request comprising the transaction number and details of credit card means entered into the virtual credit card terminal by the purchaser. While the Office Action does not map the elements of claim 13 to the teachings of Davis, Applicants assume the Office Action intended to map the virtual credit card terminal of claim 13 to the client terminal 204 of Davis, the VCT gateway of claim 13 to the payment server 206 of Davis, and the merchant of claim 13 to the merchant server 208 of Davis. As explained above, Davis teaches the merchant server 208 generates a unique identification of the transaction, not the payment server 206.

Further, as acknowledged by the Office Action, Davis fails to teach or suggest processing the VCT transaction request by the VCT gateway to facilitate formation of a bank transaction request, sending the bank transaction request from the VCT gateway to a bank, processing the bank transaction request, whereby advice is sent from the bank to the VCT gateway as to whether the transaction has been approved, and sending the advice from the VCT gateway to the merchant and the purchaser. For these elements, the Office Action cites Kuo.

Kuo



Referring to Figure 1 (reproduced right), Kuo describes an electronic commerce system with a trusted payment card host (Host 3), a computer server at a participating merchant's web site (Merchant Server 2a), and a computer client at the consumer's reach (Consumer Browser 1a) (column 5, lines 47-51). The Host 3 hosts a repository of consumers' payment cards data (column 5, lines 52-54). Consumers 1b register payment cards at a Host, or at various Hosts of their choice, and set up a pair of keys corresponding to each payment card with the Host (column 5, lines 54-57).

In a typical commercial transaction session, the Consumer 1b initiates the online transaction by sending in an order message 4 to a merchant 2b (column 6, lines 11-14). The message 4 includes ordered items, Host of choice, and an optional consumer authentication code (column 6, lines 17-18). The Host of choice is selected from a drop-down list of Hosts entrusted by the Merchant 2b (column 6, lines 21-22). The accompanying authentication code corresponds to the payment card, set up by the consumer at this selected Host 3 (column 6, lines 24-26). If the ordered items are available, the Merchant Server 2a will generate an order ID (column 6, lines 33-34). The Merchant Server may then generate an order accepted response 5a and send it to the

Consumer Browser 1a (column 6, lines 35-36). The Consumer 1b fills out a payment form and the Consumer Browser 1a generates a payment authorization request 6a and sends it to the designated Host (column 6, lines 44-60).

The Consumer Browser 1a also generates a payment-authorization-request-sent message 6c, which includes the order ID and sends it to the Merchant Server 2a (column 6, lines 60-62). Upon receiving the message 6c, the Merchant Server 2a will construct a payment approval request 7 for the order ID and send it to the Host 3 (column 6, lines 63-67). The Host 3 uses the order ID to look up the corresponding payment authorization request 6a having the same order ID (column 7, lines 14-19). The Host 3 uses the key pair and authentication code included in the payment authorization request 6a, to locate the consumer payment card data, and retrieve the payment card number (column 7, lines 34-39). The Host will then format a transaction authorization request 8a, using the payment card number and the merchant information contained in the payment approval request 7, and send it to the consumer's payment card issuer through an Internet Payment Gateway, or other payment card clearing network (column 7, lines 40-46).

If the issuer approved this transaction request, the Host 3 will generate a transaction ID (column 7, lines 55-56). This transaction ID includes the order ID and an approval code from issuer's response (column 7, lines 56-57). The Host then generates a payment-approval-request response message 10a, which includes the transaction ID and send it back to the Merchant Server (column 7, lines 65-67). The Host will also generate a payment-authorization-request 10c response message with the transaction ID, and send it back to the consumer (column 7, line 67 to column 8, line 4). After receiving the payment-approval-request response message 10a from the Host 3, the Merchant Server will generate a fulfillment request 11, which includes the order ID and those ordered items to be fulfilled, and sent the fulfillment request 11 to the merchant's fulfillment department (column 8, lines 6-12). Upon completion of order fulfillment, a fulfillment ID 12 is generated and sent to the Merchant Server 2a (column 8, lines 12-15). Then, the Merchant Server 2a generates an order-fulfilled response message 13b, and send it to the consumer (column 8, lines 18-21).

A payment capturing request 13a is generated, which includes the transaction ID and

money amount, and sent back to the Host 3 (column 8, lines 22-24). Upon receiving the payment capturing request 13a, the Host will verify the money amount against data stored under the transaction ID (column 8, lines 25-27). If the money amount and transaction ID are validated by the Host, before the record expires, the Host 3 will generate a transaction clearing request 14a, and send it to the payment card issuer, via an Internet Payment Gateway, or a payment card clearing network (column 8, lines 36-42). Upon receiving the transaction-clearing-request response 15 from the consumer's payment card issuer, the Host 3 will generate a payment-capturing-request response message 16, which includes the transaction ID, and send it back to the Merchant Server 2a (column 8, lines 42-47). This completes the transaction (column 8, lines 47-49).

Thus, the Host 3 of Kuo generates a transaction ID after the issuer approved the transaction request. Therefore, this transaction ID cannot be included in the VCT transaction request as recited in claim 13. Further, Kuo does not teach or suggest that the transaction ID is sent from the purchaser to the Host. Kuo also fails to teach or suggest that a request for a transaction number is received from the merchant. Instead, Kuo teaches the transaction ID is generated when the issuer approved the transaction request.

The system of Kuo differs significantly from the system of Davis. Specifically, the system of Davis is for use with a stored-value card 5 read by a card reader 210 at the time of the transaction. In contrast, Kuo teaches a system in which payment card data is stored on a trusted Host 3 and accessed using keys created when the payment cards are registered with the host. Because Davis uses stored-value cards, when one of the security cards 218 and 220 authenticates and validates the user's stored-value card 5, the value stored by the card may be debited at the time of the transaction and the transactions collected and sent to a clearing and administration system for processing in batches. In contrast, in Kuo, the transaction authorization request 8a is sent to authorize a transaction then, after order fulfillment, the Host 3 sends a transaction clearing request 14a to the payment card issuer, via an Internet Payment Gateway, or a payment card clearing network for the order.

Mertens

Mertens discloses a system 100 including a client 110, a merchant 120, and a credit card company/agent 130, all of which are connected via the Internet 102 (page 2, paragraph 24). In an alternate embodiment, illustrated in Figure 4, Mertens discloses a system 150 including a client 160, a merchant 190 and a credit card company/authorizing agent 180, all of which are connected via the Internet 102 (page 2, paragraph 28). Thus, Mertens is completely silent with respect to a VCT gateway. Therefore, Mertens cannot cure the deficiencies of Davis and Kuo discussed above.

Davis, Kuo, and Mertens

For at least the reasons discussed above, Davis, Kuo, and Mertens alone and in hypothetical combination fail to teach or suggest the invention of claim 13 and claims 14, 15, and 17-24 that depend from claim 13. Withdrawal of this ground for rejection is respectfully requested.

New Claim 25

New claim 25 recites a method performed by a virtual credit card terminal (VCT) gateway connected to a financial institution, a merchant computing device, and a purchaser computing device, the purchaser computing device being operatively coupled to a credit card reader to receive payment information read thereby. The method includes receiving a request for a transaction number from the merchant computing device after the merchant computing device has received order information and payment information from the purchaser computing device. The method also includes receiving a VCT transaction request from the purchaser computing device, the VCT transaction request comprising the transaction number, the transaction amount, and the payment information received by the purchaser computing device from the credit card reader. In response to the VCT transaction request, a payment approval request is sent to the financial institution requesting approval to charge the transaction amount to the account associated with the payment information. As explained above, Davis, Kuo, and Mertens alone and in hypothetical

combination fail to teach or suggest these elements. Therefore, new claim 25 is allowable over the cited references.

In conclusion

Applicants contend that all claims are allowable. The Examiner is encouraged to phone Applicants' attorney, Barry L. Davison, to resolve any outstanding issues and expedite allowance of this application.

Davis Wright Tremaine LLP
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: 206-757-8023
Fax: 206-757-7023

Respectfully submitted,
Gregory John Litster et al.
Davis Wright Tremaine LLP

/Barry L. Davison, Ph.D., J.D./
Barry L. Davison, Ph.D., J.D.
Attorney for Applicant
Registration No. 47,309